

1 **CLAIMS**

2 1. A method comprising:

3 presenting a user with a plurality of modes of operation, wherein the
4 plurality of modes of operation define different trust options for handling sensitive
5 data associated with the user;

6 receiving a selection from the user, wherein the selection is one of the
7 plurality of modes of operation; and

8 handling sensitive data associated with the user in accordance with the
9 selected mode of operation.

10
11 2. A method as recited in claim 1 wherein the plurality of modes include
12 a low trust option for handling sensitive data associated with the user, the low trust
13 option configured to retrieve sensitive data from the user each time the user
14 requests a service requiring the sensitive data.

15
16 3. A method as recited in claim 2 wherein the low trust option does not
17 persistently store sensitive data after the requested service requiring the sensitive
18 data has been completed.

19
20 4. A method as recited in claim 1 wherein the plurality of modes include
21 a high trust option for handling sensitive data associated with the user, the high
22 trust option configured to retrieve sensitive data from the user and store the
23 sensitive data in an encrypted format for future use.

1 5. A method as recited in claim 1 wherein the plurality of modes include
2 a high trust option for handling sensitive data associated with the user, the high
3 trust option configured to retrieve sensitive data from the user, encode the
4 sensitive data using a two-way encryption technique, and store the encrypted
5 sensitive data.

6
7 6. A method as recited in claim 1 wherein the plurality of modes include
8 a moderate trust option for handling sensitive data associated with the user, the
9 moderate trust option configured to retrieve sensitive data from the user and store
10 the sensitive data in an encrypted format using a password known only to the user.

11
12 7. A method as recited in claim 1 wherein the plurality of modes include
13 a moderate trust option for handling sensitive data associated with the user, the
14 moderate trust option configured to retrieve sensitive data from the user, encode
15 the sensitive data using a one-way encryption technique, and store the encrypted
16 sensitive data.

17
18 8. A method as recited in claim 1 further comprising assigning a default
19 mode of operation if the user does not select a valid mode of operation.

20
21 9. A method as recited in claim 1 further comprising associating a user
22 account with the selected mode of operation.

1 **10.** A method comprising:

2 presenting a user with a low trust mode of operation, wherein the low trust
3 mode of operation retrieves sensitive data from the user each time the user
4 requests a service requiring the sensitive data;

5 presenting the user with a high trust mode of operation, wherein the high
6 trust mode of operation stores sensitive data received from the user in an
7 encrypted format;

8 receiving a selection from the user indicating one of the two modes of
9 operation; and

10 handling sensitive data associated with the user in accordance with the
11 selected mode of operation.

12
13 **11.** A method as recited in claim 10 further comprising presenting the
14 user with a moderate trust mode of operation, wherein the moderate trust mode of
15 operation stores sensitive data from the user in an encrypted format using a
16 password known to the user; and wherein receiving a selection from the user
17 includes receiving a selection indicating one of the three modes of operation.

18
19 **12.** A method as recited in claim 10 further comprising associating a
20 user account with the selected mode of operation.

21
22 **13.** A method as recited in claim 10 further comprising assigning a
23 default trust mode if the user does not select a valid mode of operation.

1 **14.** One or more computer-readable memories containing a computer
2 program that is executable by a processor to perform the method recited in claim
3 10.
4

5 **15.** A method comprising:

6 presenting a user with a moderate trust mode of operation, wherein the
7 moderate trust mode of operation stores sensitive data from the user in an
8 encrypted format using a password known to the user;

9 presenting the user with a high trust mode of operation, wherein the high
10 trust mode of operation stores sensitive data received from the user;

11 receiving a selection from the user indicating one of the two modes of
12 operation; and

13 handling sensitive data associated with the user in accordance with the
14 selected mode of operation.

15
16 **16.** One or more computer-readable memories containing a computer
17 program that is executable by a processor to perform the method recited in claim
18 15.
19
20
21
22
23
24
25

1 **17.** A method comprising:

2 presenting a user with a moderate trust mode of operation, wherein the
3 moderate trust mode of operation stores sensitive data from the user in an
4 encrypted format using a password known to the user;

5 presenting the user with a low trust mode of operation, wherein the low
6 trust mode of operation retrieves sensitive data from the user each time the user
7 requests a service requiring the sensitive data;

8 receiving a selection from the user indicating one of the two modes of
9 operation; and

10 handling sensitive data associated with the user in accordance with the
11 selected mode of operation.

12
13 **18.** One or more computer-readable memories containing a computer
14 program that is executable by a processor to perform the method recited in claim
15 17.

1 **19.** One or more computer-readable media having stored thereon a
2 computer program that, when executed by one or more processors, causes the one
3 or more processors to:

4 present a user with a plurality of modes of operation, wherein the plurality
5 of modes of operation define different trust options for handling sensitive data
6 associated with the user;

7 receive a selection from the user, wherein the selection is one of the
8 plurality of modes of operation; and

9 process sensitive data associated with the user in accordance with the
10 selected mode of operation.

11
12 **20.** One or more computer-readable media as recited in claim 19
13 wherein the plurality of modes of operation include a low trust option for handling
14 sensitive data associated with the user, the low trust option configured to retrieve
15 sensitive data from the user each time the user requests a service requiring the
16 sensitive data.

17
18 **21.** One or more computer-readable media as recited in claim 20
19 wherein the low trust option does not persistently store sensitive data after the
20 requested service requiring the sensitive data is complete.

1 **22.** One or more computer-readable media as recited in claim 19
2 wherein the plurality of modes of operation include a high trust option for
3 handling sensitive data associated with the user, the high trust option configured to
4 retrieve sensitive data from the user and store the sensitive data in an encrypted
5 format.

6

7 **23.** One or more computer-readable media as recited in claim 19
8 wherein the plurality of modes of operation include a moderate trust option for
9 handling sensitive data associated with the user, the moderate trust option
10 configured to retrieve sensitive data from the user and store the sensitive data in an
11 encrypted format using a password known only to the user.

12
13
14
15
16
17
18
19
20
21
22
23
24
25